Appendix D

Use of Passwords with CT

D-1. CT Passwords

The CT uses passwords to limit access to different setups, functions, and levels of classified material processed and stored by the CT. Password control allows the CT owner to permit certain individuals access to different levels of classified material and to make changes to the operating parameters without giving all operators access to TOP SECRET material.

There are nine passwords used in the CT. These passwords control access to such functions as changing the GUARDED menu, enabling different classification levels for the terminal, changing the PLA/RI table, setting different passwords for the classification level of the operators, transmitting messages, and entering the Disk Operating System (DOS).

Passwords are critical to the CT security. Persons having passwords must be instructed on password sensitivity, protection, and personal responsibility for their security. For security reasons, passwords will be treated as more valuable than safe combinations.

Functions which require one or more passwords to access them are listed below.

DOS. The password to access DOS should be limited to a minimum number of personnel as it is not required for routine message processing.

GUARDED. The password to access this function must be strictly controlled and issued to a minimum number of personnel. The GUARDED menu is where initialization items are entered or changed and where the PLA/RI table is updated (additional password is required for this function).

ENABLE. The password to access the ENABLE function will be strictly controlled and issued only to those personnel requiring specific access. All personnel who are authorized to compose messages for a given level of classification will have the same password for this function. A different password is used for each level of access with a user having automatic access to all classifications at or lower than what they are authorized. Access to SECRET means the user can access SECRET and CONFIDENTIAL but not TOP SECRET.

PLA/RI. The password to access this function will be controlled by the security manager. The PLA/RI password is used to add, delete, and make changes to the PLA/RI table.

SET PASS. The password to access this function is limited to CT personnel with a TOP SECRET clearance and a need to know. This password allows the CT manager to change any of the current passwords prior to changing to new passwords.

D-2. CT Password Control

The security manager or ISS0 is responsible for the generation, issuance, and control of all system passwords, CT passwords require the following procedures to be in effect:

- Randomly generated (never common words or phrases).
- Classify at the highest level as the granted access.
- Require strict receipt procedures.
- Change at least semiannually or upon departure of an individual having knowledge of a password.

Password generation and control is outlined in paragraph 2-15 of AR 380-19.

The CT manager, using stringent password control, will be able to limit access to the different CT functions. Restricted access will reduce the possibility of unauthorized parameter alterations, and compromise of information, while still allowing multiple users to process outgoing and incoming record traffic efficiently.